APPENDIX A

Tutorials

Understanding 802.11 Frame Types

By Jim Geier

When analyzing or troubleshooting the operation of a wireless LAN, you'll likely be using an 802.11 packet analyzer (e.g., AiroPeek or Sniffer Wireless) to monitor the communications between radio network interface cards (NICs) and access points. After capturing the packets, you need to understand the different 802.11

frame types as a basis for deciphering what the network is or isn't doing. In this tutorial, I'll give you an overview of the more common 802.11 frames to help you become more adept at comprehending the operation of a wireless LAN and solving network problems.

General frame concepts

RELATED ARTICLES

802.11 Alphabet Soup

Beating Signal Loss in WLANs

EIRP Limitations for 802.11 WLANs

The 802.11 standard defines various frame types that stations (NICs and access points) use for communications, as well as managing and controlling the wireless link. Every frame has a control field that depicts the 802.11 protocol version, frame type, and various indicators, such as whether WEP is on, power management is active, and so on. In addition all frames contain MAC addresses of the source and destination station (and access point), a frame sequence number, frame body and frame check sequence (for error detection).

802.11 data frames carry protocols and data from higher layers within the frame body. A data frame, for example, could be carrying the HTML code from a Web page (complete with TCP/IP headers) that the user is viewing. Other frames that stations use for management and control carry specific information regarding the wireless link in the frame body. For example, a beacon's frame body contains the service set identifier (SSID), timestamp, and other pertinent information regarding the access point.

Note: For more details regarding 802.11 frame structure and usage, refer to the 802.11 standard, which is free for download from the 802.11 Working Group Web site.

Management Frames

802.11 management frames enable stations to establish and maintain communications. The following are common 802.11 management frame subtypes:

- **Authentication frame:** 802.11 authentication is a process whereby the access point either accepts or rejects the identity of a radio NIC. The NIC begins the process by sending an authentication frame containing its identity to the access point. With open system authentication (the default), the radio NIC sends only one authentication frame, and the access point responds with an authentication frame as a response indicating acceptance (or rejection). With the optional shared key authentication, the radio NIC sends an initial authentication frame, and the access point responds with an authentication frame containing challenge text. The radio NIC must send an encrypted version of the challenge text (using its WEP key) in an authentication frame back to the access point. The access point ensures that the radio NIC has the correct WEP key (which is the basis for authentication) by seeing whether the challenge text recovered after decryption is the same that was sent previously. Based on the results of this comparison, the access point replies to the radio NIC with an authentication frame signifying the result of authentication.

- **Deauthentication frame:** A station sends a deauthentication frame to another station if it wishes to terminate secure communications.

- **Association request frame:** 802.11 association enables the access point to allocate resources for and synchronize with a radio NIC. A NIC begins the association process by sending an association request to an access point. This frame carries information about the NIC (e.g., supported data rates) and the SSID of the network it wishes to associate with. After receiving the association request, the access point considers associating with the NIC, and (if accepted) reserves memory space and establishes an association ID for the NIC.

- **Association response frame:** An access point sends an association response frame containing an acceptance or rejection notice to the radio NIC requesting association. If the access point accepts the radio NIC, the frame includes information regarding the association, such as association ID and supported data rates. If the outcome of the association is positive, the radio NIC can utilize the access point to communicate with other NICs on the network and systems on the distribution (i.e., Ethernet) side of the access point.

- **Reassociation request frame:** If a radio NIC roams away from the currently associated access point and finds another access point having a stronger beacon signal, the radio NIC will send a reassociation frame to the new access point. The new access point then coordinates the forwarding of data frames that may still be in the buffer of the previous access point waiting for transmission to the radio NIC.

- **Reassociation response frame:** An access point sends a reassociation response frame containing an acceptance or rejection notice to the radio NIC requesting reassociation. Similar to the association process, the frame includes information regarding the association, such as association ID and supported data rates.

- **Disassociation frame:** A station sends a disassociation frame to another station if it wishes to terminate the association. For example, a radio NIC that is shut down gracefully can send a disassociation frame to alert the access point that the NIC is powering off. The access point can then relinquish memory allocations and remove the radio NIC from the association table.

- **Beacon frame:** The access point periodically sends a beacon frame to announce its presence and relay information, such as timestamp, SSID, and other parameters regarding the access point to radio NICs that are within range. Radio NICs continually scan all 802.11 radio channels and listen to beacons as the basis for choosing which access point is best to associate with.

- **Probe request frame:** A station sends a probe request frame when it needs to obtain information from another station. For example, a radio NIC would send a probe request to determine which access points are within range.

- **Probe response frame:** A station will respond with a probe response frame, containing capability information, supported data rates, etc., when after it receives a probe request frame.

Control Frames

802.11 control frames assist in the delivery of data frames between stations. The following are common 802.11 control frame subtypes:

- **Request to Send (RTS) frame:** The RTS/CTS function is optional and reduces frame collisions present when hidden stations have associations with the same access point. A station sends a RTS frame to another station as the first phase of a two-way handshake necessary before sending a data frame.

- **Clear to Send (CTS) frame:** A station responds to a RTS with a CTS frame, providing clearance for the requesting station to send a data frame. The CTS includes a time value that causes all other stations (including hidden stations) to hold off transmission of frames for a time period necessary for the requesting station to send its frame. This minimizes collisions among hidden stations, which can result in higher throughput if you implement it properly.

- **Acknowledgement (ACK) frame:** After receiving a data frame, the receiving station will utilize an error checking processes to detect the

presence of errors. The receiving station will send an ACK frame to the sending station if no errors are found. If the sending station doesn't receive an ACK after a period of time, the sending station will retransmit the frame.

Data Frames

Of course the main purpose of having a wireless LAN is to transport data. 802.11 defines a data frame type that carries packets from higher layers, such as web pages, printer control data, etc., within the body of the frame. When viewing 802.11 data frames with a packet analyzer, you can generally observe the contents of the frame body to see what packets that the 802.11 data frames are transporting.

Jim Geier provides independent consulting services to companies developing and deploying wireless network solutions. He is the author of the book, Wireless LANs *(SAMs, 2001), and regularly instructs workshops on wireless LANs. Join Jim for discussions as he answers questions in the 802.11 Planet Forums.*

August 15, 2002

RELATED ARTICLES

802.11 Alphabet Soup

Beating Signal Loss in WLANs

EIRP Limitations for 802.11 WLANs

Email this article to a colleague

Go to a printable version of this story